

WHAT IS CLAIMED IS:

- 1 1. A group formation/management system, comprising:
 - 2 one or more registered member devices operable to hold
 - 3 common secret information unique to a group;
 - 4 a new member device operable to transmit a request for
 - 5 registration to the group, and to receive and hold the common
 - 6 secret information; and
 - 7 a group management device operable to receive the
 - 8 registration request from the new member device, and when
 - 9 a registered number of member devices is less than a maximum
 - 10 number of member devices registerable in the group, to
 - 11 register the new member device and output the common secret
 - 12 information to the new member device.

- 1 2. A group formation/management system, comprising: ~
 - 2 a member device operable to transmit a request for
 - 3 registration to a group, and to receive and hold common secret
 - 4 information unique to the group; and
 - 5 a group management device operable to receive the
 - 6 registration request from the member device, and when a
 - 7 registered number of member devices is less than a maximum
 - 8 number of member devices registerable in the group, to
 - 9 register the member device and output the common secret
 - 10 information to the member device, wherein

11 in an initial state, the group has no member devices
12 registered therein.

1 3. A group management device that manages a group,
2 comprising:

3 a reception unit operable to receive from a member
4 device, a request for registration to the group;

5 a judging unit operable, if the member device is
6 authenticated as being a legitimate device, to judge whether
7 a registered number of member devices is less than a maximum
8 number of member devices registerable in the group, and to
9 register the member device when judged in the affirmative;
10 and

11 a communication unit operable, when the judging unit
12 judges in the affirmative, to output to the member device,
13 common secret information unique to the group.

1 4. The group management device of claim 3, wherein

2 the judging unit includes:

3 an authentication subunit operable to hold a second
4 initial value, and to authenticate the member device, using
5 the second initial value and a first initial value held by
6 the member device; and

7 a device-number judging subunit operable, when

8 authentication is successful, to judge whether the
9 registered number is less than the maximum number,
10 the common secret information outputted by the
11 communication unit shows "registered in the group", and
12 the member device receives and holds the outputted
13 common secret information, and deactivates the first initial
14 value.

1 5. The group management device of claim 4, wherein
2 the first and second initial values show "unregistered
3 in the group".

1 6. The group management device of claim 4, wherein
2 the first and second initial values show "unregistered
3 in any group".

1 7. The group management device of claim 3, further
2 comprising:
3 a generating unit operable to generate the common
4 secret information, wherein
5 the communication unit outputs the generated common
6 secret information to the member device.

1 8. The group management device of claim 3, wherein

2 the common secret information is generated by a
3 management device outside of the group,
4 the judging unit receives the common secret information
5 from the out-group management device, and
6 the communication unit outputs the received common
7 secret information to the member device.

1 9. The group management device of claim 3, wherein
2 the reception unit, on receipt of the registration
3 request, notifies the receipt to a management device outside
4 of the group,
5 the out-group management device judges whether the
6 registered number is less than the maximum number,
7 the judging unit, instead of judging whether the
8 registered number is less than the maximum number, receives
9 a judgment result from the out-group management device, and
10 the communication unit outputs the common secret
11 information to the member device, when the judgment result
12 shows that the registered number is less than the maximum
13 number.

1 10. The group management device of claim 3, wherein
2 the maximum number is formed from a first maximum number
3 and a second maximum number, and

4 the judging unit judges whether the registered number
5 is less than one of the first maximum number and the second
6 maximum number, and registers the member device when judged
7 in the affirmative.

1 11. The group management device of claim 10, wherein

2 the first maximum number is the number of member devices,
3 out of the maximum number, connectable to the group
4 management device, and the second maximum number is the
5 number of member devices, out of the maximum number, not
6 connectable to the group management device, and

7 the judging unit judges, (i) when the member device is
8 connectable to the group management device, whether the
9 registered number of connectable member devices is less than
10 the first maximum number, and (ii) when the member device
11 is not connectable to the group management device, whether
12 the registered number of non-connectable member devices is
13 less than the second maximum number.

1 12. The group management device of claim 3, wherein

2 the communication unit outputs to another group
3 management device, a request inquiring whether the member
4 device is registerable in the other group management device,
5 the other group management device receives the inquiry

6 request, judges whether a registered number of member devices
7 is less than a maximum number of member devices registerable
8 with the other group management device, and when judged in
9 the affirmative, registers the member device and outputs the
10 common secret information to the group management device,
11 and

12 the communication unit, on receipt of the common secret
13 information from the other group management device, outputs
14 the received common secret information to the member device.

1 13. The group management device of claim 3, wherein
2 the judging unit functions to resist invalid access
3 from outside, and
4 the maximum number and the common secret information
5 are stored in an area that is unreadable/unwritable from
6 outside.

1 14. The group management device of claim 13, wherein
2 the judging unit is included in a portable module that
3 is mountable in the group management device.

1 15. The group management device of claim 3, wherein
2 the judging unit stores a remaining number obtained by
3 subtracting the registered number from the maximum number,

4 and on receipt by the reception unit of the registration
5 request, judges whether the remaining number is "0", and when
6 judged that the remaining number is not "0", the
7 communication unit outputs the common secret information to
8 the member device and the judging unit subtracts "1" from
9 the remaining number.

1 16. The group management device of claim 3, wherein
2 the reception unit, after the outputting of the common
3 secret information, receives from the member device, a
4 request for withdrawal from the group,
5 the communication unit, on receipt by the reception
6 unit of the withdrawal request, outputs to the member device,
7 a notification indicating to delete the common secret
8 information,
9 the reception unit receives from the member device, a
10 notification showing that deletion of the common secret
11 information has been completed, and
12 the judging unit, on receipt by the reception unit of
13 the deletion-completed notification, reduces the registered
14 number.

1 17. The group management device of claim 3, wherein
2 the judging unit, when judged that the registered

3 number is less than the maximum number, issues information
4 showing a valid period during which use of the common secret
5 information is permitted in the member device, increases the
6 registered number, monitors the elapse of the valid period,
7 and reduces the registered number when the valid period ends,
8 and
9 the communication unit outputs the issued information
10 to the member device.

1 18. The group management device of claim 3, wherein
2 the judging unit receives from a management device
3 outside of the group, a number of member devices registerable
4 in the group, pays an accounting fee in accordance with the
5 received number, and sets the received number as the maximum
6 number.

1 19. The group management device of claim 3, wherein
2 the judging unit newly acquires from a management
3 device outside of the group, a number of member devices
4 registerable in the group, pays an accounting fee in
5 accordance with the acquired number, and adds the acquired
6 number to the maximum number to obtain a new maximum number.

1 20. The group management device of claim 3, wherein

2 the reception unit, after the outputting of the common
3 secret information, receives a communication request from
4 the member device,

5 the judging unit authenticates the member device using
6 the common secret information and common secret information
7 held by the member device, and

8 the communication unit communicates with the member
9 device when authentication is successful.

1 21. The group management device of claim 3, further
2 comprising:

3 a content storage unit operable to store therein a
4 content key and an encrypted content encrypted using the
5 content key; and

6 an encryption unit operable to encrypt the content key
7 using a key generated based on the common secret information,
8 to generate an encrypted content key, wherein

9 the communication unit outputs the encrypted content
10 and the encrypted content key to the member device.

1 22. The group management device of claim 21, wherein

2 the judging unit authenticates the member device using
3 the common secret information and common secret information
4 held by the member device, and shares a session key with the

5 member device, using the common secret information, and
6 the encryption unit, when authentication is successful,
7 encrypts the content key using the shared session key.

1 23. The group management device of claim 3, wherein
2 the communication unit stores therein the common secret
3 information, newly receives a different piece of common
4 secret information, overwrites the stored common secret
5 information with the newly received common secret
6 information, and outputs, regularly or irregularly, the
7 newly received common secret information to the member
8 device.

1 24. The group management device of claim 3, further
2 comprising:
3 a content storage unit operable to store therein a
4 content key and an encrypted content encrypted using the
5 content key;
6 an encryption unit operable to encrypt the content key
7 using a key generated based on the common secret information,
8 to generate an encrypted content key; and
9 a writing unit operable to write the encrypted content
10 and the encrypted content key to a portable recordable
11 medium.

1 25. The group management device of claim 24, wherein
2 the received registration request includes an
3 identifier identifying the member device, and
4 the encryption unit encrypts the content key using a
5 key generated based on the common secret information and the
6 identifier, to generate the encrypted content key.

1 26. The group management device of claim 24,
2 the encryption unit encrypts the content key using a
3 key generated based on the common secret information and an
4 identifier unique to the portable recordable medium.

1 27. The group management device of claim 3, further
2 including:

3 a holding unit operable to hold, in correspondence with
4 identifiers that each identify a different group, (i) common
5 secret information unique to the group and (ii) a maximum
6 number of member devices registerable in the group, wherein
7 the received registration request includes one of the
8 identifiers,

9 the judging unit, on receipt by the reception unit of
10 the registration request, judges whether the number of member
11 devices registered in a group identified by the identifier
12 is less than a maximum number corresponding to the identifier,

13 and when judged in the affirmative, registers the member
14 device in the group and selects common secret information
15 corresponding to the identifier, and
16 the communication unit outputs the selected common
17 secret information to the member device.

1 28. The group management device of claim 3, wherein
2 the received registration request requests the
3 registration of a predetermined number of other member
4 devices,
5 the judging unit judges whether an aggregate number
6 obtained by adding the predetermined number to the registered
7 number is less than the maximum number, and when judged in
8 the affirmative, generates a permission right permitting a
9 copying of the common secret information to the predetermined
10 number of member devices, and
11 the permission right is attached to the outputted
12 common secret information.

1 29. The group management device of claim 3, wherein
2 the received registration request includes a first
3 identifier unique to the member device,
4 the judging unit stores therein the first identifier,
5 the reception unit, after the outputting of the common

6 secret information, receives a second identifier unique to
7 the member device,
8 the judging unit judges whether the second identifier
9 matches the first identifier, and
10 the communication unit, when judged that the first and
11 second identifiers match, again outputs the common secret
12 information to the member device.

1 30. The group management device of claim 3, wherein
2 when the group management device is determined to be
3 a new group management device for managing a new group formed
4 by combining groups managed by a plurality of group
5 management devices, the communication unit outputs to member
6 devices registered in the groups, new common secret
7 information unique to the new group, and
8 when one of the other group management devices is
9 determined to be the new group management device, the group
10 management device further comprises:
11 a receiving unit operable to receive the new common
12 secret information from the other group management device;
13 and
14 a holding unit operable to hold the received new common
15 secret information.

1 31. The group management device of claim 30, wherein
2 the communication unit determines in conjunction with
3 the other group management devices, one of the group
4 management devices to be the new group management device.

1 32. The group management device of claim 31, wherein
2 the holding unit stores therein a priority level of the
3 group management device, and
4 the communication unit determines, out of the stored
5 priority level and priority levels of the other group
6 management devices, the group management device having the
7 highest priority level to be the new group management device.

1 33. The group management device of claim 30, wherein
2 each member device registered in the groups managed by
3 the group management device and the other group management
4 devices has a priority level, and
5 when the group management device is determined to be
6 the new group management device, the reception unit acquires
7 the priority levels of the member devices,
8 the group management device further comprises a
9 selecting unit operable to select, in order from highest to
10 lowest of the acquired priority levels, member devices for
11 registration in the new group, the selected number of member

12 devices being less than or equal to a maximum number of member
13 devices registerable in the new group, and
14 the communication unit outputs the new common secret
15 information to the selected member devices.

1 34. The group management device of claim 3, further
2 comprising:

3 a determining unit operable, after the outputting of
4 the common secret information, to determine a member device
5 registered in the group to be another group management
6 device; and

7 a dividing unit operable to divide member devices
8 registered in the group into member devices to be registered
9 in a group managed by the group management device and member
10 devices to be registered in another group managed by the other
11 group management device, and

12 the communication unit outputs, after the dividing by
13 the dividing unit, a different piece of common secret
14 information to the member devices to be registered in the
15 group managed by the group management device.

1 35. A member device that uses a content after registering λ
2 in a group managed by a group management device, comprising:
3 a requesting unit operable to request the group

4 management device for registration to the group;
5 a receiving unit operable to be authenticated by the
6 group management device, and to receive from the group
7 management device, common secret information unique to the
8 group; and
9 a holding unit operable to hold the received common
10 secret information.

1 36. The member device of claim 35, wherein
2 the holding unit holds a first initial value,
3 the receiving unit is authenticated by the group
4 management device using the first initial value, and receives
5 the common secret information from the group management
6 device when authentication is successful, and
7 the holding unit deactivates the first initial value
8 and holds the received common secret information.

1 37. The member device of claim 36, wherein
2 the first initial value shows "unregistered in the
3 group".

1 38. The member device of claim 36, wherein
2 the first initial value shows "unregistered in any
3 group".

1 39. The member device of claim 36, wherein
2 the holding unit overwrites the first initial value
3 with the common secret information.

1 40. The member device of claim 36, further comprising:
2 a communication unit operable, after the holding of the
3 common secret information, to output the common secret
4 information to another member device; and
5 a deletion unit operable to delete the held common
6 secret information after the outputting by the communication
7 unit, wherein
8 the holding unit reactivates the first initial value
9 after the deleting by the deletion unit.

1 41. The member device of claim 36, wherein
2 the requesting unit requests the group management
3 device for withdrawal from the group,
4 the receiving unit receives from the group management
5 device, a notification indicating to delete the common secret
6 information, and
7 the holding unit deletes the held common secret
8 information and reactivates the first initial value.

1 42. The member device of claim 35, wherein

2 the receiving unit, after the holding of the common
3 secret information, newly receives a different piece of
4 common secret information from the group management device,
5 and

6 the holding unit overwrites the held common secret
7 information with the newly received common secret
8 information.

1 43. The member device of claim 35, wherein

2 the requesting unit requests the group management
3 device for delivery of the content,

4 the receiving unit receives from the group management
5 device, an encrypted content generated by encrypting the
6 content using a content key, and an encrypted content key
7 generated by encrypting the content key using an encryption
8 key generated based on the common secret information, and

9 the member device further comprises a decryption unit
10 operable to generate a decryption key the same as the
11 encryption key, based on the common secret information, to
12 decrypt the encrypted content key using the decryption key
13 to obtain a content key, and to decrypt the encrypted content
14 using the content key to obtain a content.

1 44. The member device of claim 35, wherein

2 the holding unit includes a storage subunit that is
3 unreadable/unwritable from outside, and
4 the storage subunit stores therein the received common
5 secret information.

1 45. The member device of claim 44, wherein
2 the storage subunit is a recording medium mountable in
3 the member device.

1 46. The member device of claim 35, further comprising:
2 an authentication unit operable, after the holding of
3 the common secret information, and when the member device
4 communicates with another member device, to authenticate the
5 other member device using the held common secret information
6 and common secret information held by the other member
7 device.

1 47. The member device of claim 35, further comprising:
2 a communication unit operable, after the holding of the
3 common secret information, to output the common secret
4 information to another member device; and
5 a deletion unit operable to delete the held common
6 secret information after the outputting by the communication
7 unit.

1 48. The member device of claim 35, wherein:

2 the requesting unit requests the group management
3 device for withdrawal from the group,

4 the receiving unit receives from the group management
5 device, a notification indicating to delete the common secret
6 information, and

7 the holding unit, on acquisition of the deletion
8 notification by the receiving unit, deletes the held common
9 secret information.

1 49. The member device of claim 35, wherein

2 the received common secret information includes
3 information showing a valid period during which use of the
4 common secret information is permitted in the member device,
5 and

6 the holding unit monitors an elapse of the valid period
7 and deletes the common secret information when the valid
8 period ends.

1 50. The member device of claim 35, wherein

2 the requesting, receiving and holding units are
3 included in a portable module that is mountable in the member
4 device and the group management device, and

5 the receiving unit receives the common secret

6 information from the group management device, when the
7 portable module is mounted in the group management device.

1 51. The member device of claim 50, wherein

2 the receiving unit receives from the group management
3 device, an encrypted content encrypted using a content key,
4 and an encrypted content key generated by encrypting the
5 content key using an encryption key generated based on the
6 common secret information, and

7 the member device further comprises:

8 a decryption unit operable to read the common secret
9 information from the mounted portable module, generate a
10 decryption key the same as the encryption key, based on the
11 read common secret information, decrypt the encrypted
12 content key using the decryption key to obtain a content key,
13 and decrypt the encrypted content using the content key to
14 obtain a content.

1 52. The member device of claim 50, wherein

2 the portable module further includes:

3 a notifying unit operable, when the portable module is
4 mounted in the member device, to notify the held common secret
5 information to the member device; and

6 a management unit operable, after the notifying of the

7 held common secret information, to prohibit the notifying
8 unit from again notifying the held common secret information
9 to the member device, and

10 the member device further comprises a storage unit
11 operable to receive and store therein the common secret
12 information notified from the portable module.

1 53. The member device of claim 35, wherein

2 the holding unit holds a maximum holdable number, which
3 is the number of pieces of common secret information holdable
4 by the holding unit, and

5 the requesting unit requests the group management
6 device for registration to the group when the number of pieces
7 of held common secret information is less than the maximum
8 holdable number.

1 54. The member device of claim 53, wherein

2 the holding unit holds identifiers that each identify
3 a different group,

4 the registration request includes one of the
5 identifiers, and

6 the holding unit holds the received common secret
7 information in correspondence with the identifier included
8 in the registration request.

1 55. The member device of claim 35, wherein
2 the requesting unit requests the group management
3 device for registration of a predetermined number of other
4 member devices,
5 the received common secret information has attached a
6 permission right permitting a copying of the common secret
7 information to the predetermined number of member devices,
8 the member device further comprises a communication
9 unit operable to output the common secret information to
10 another member device, and
11 the holding unit reduces the number of copies permitted
12 by the permission right by "1" when the common secret
13 information is outputted by the communication unit.

1 56. The member device of claim 55, wherein
2 the holding unit holds an identifier unique to the
3 member device,
4 the communication unit acquires from the other member
5 device, an identifier unique to the other member device, and
6 the requesting unit transmits the held and acquired
7 identifiers to the group management device.

1 57. The member device of claim 35, wherein
2 the holding unit holds an identifier unique to the

3 member device,
4 the registration request includes the identifier,
5 the holding unit, on receipt of a power-OFF instruction,
6 deletes the held common secret information and sets power
7 off, and
8 on receipt of a power-ON instruction, the requesting
9 unit again transmits the identifier to the group management
10 device, and the receiving unit again receives the common
11 secret information from group management device.

1 58. The member device of claim 35, wherein
2 the holding unit holds an identifier unique to the
3 member device,
4 the registration request includes the identifier,
5 the holding unit, when communication with the group
6 management device is interrupted, deletes the held common
7 secret information, and
8 when communication with the group management device is
9 reestablished, the requesting unit again transmits the
10 identifier to the group management device, and the receiving
11 unit again receives the common secret information from group
12 management device.

1 59. The member device of claim 35, wherein

2 the receiving unit, after the holding of the common
3 secret information, newly receives a different piece of
4 common secret information from one of the group management
5 device and another group management device, and

6 the holding unit deactivates the held common secret
7 information and holds the newly received common secret
8 information.

1 60. The member device of claim 35, further comprising:

2 a dividing unit operable, after the holding of the
3 common secret information, and when the member device is
4 determined by the group management device to be another group
5 management device, to divide member devices registered in
6 the group into member devices to be registered in a group
7 managed by the group management device and member devices
8 to be registered in another group managed by the other group
9 management device; and

10 a communication unit operable to output to the member
11 devices to be registered in the other group, common secret
12 information unique to the other group.

1 61. The member device of claim 60, wherein

2 the member devices registered in the group each have
3 a priority level,

4 the receiving unit acquires the priority levels of the
5 other member devices, and

6 the dividing unit conducts the dividing based on the
7 acquired priority levels.

1 62. A registration device that registers a member device in
2 a group managed by a group management device, comprising:

3 a holding unit operable to receive from the group
4 management device and hold, common secret information unique
5 to the group; and

6 a notifying unit operable, when the registration device
7 is connected to the member device, to notify the common secret
8 information to the member device.

1 63. The registration device of claim 62, further comprising:

2 a management unit operable, after the notifying of the
3 common secret information, to prohibit the notifying unit
4 from again notifying the common secret information to the
5 member device.

1 64. The registration device of claim 62, further comprising:

2 a reception unit operable to receive from the member
3 device, a request for acquisition of the common secret
4 information, wherein

5 the notifying unit notifies the common secret
6 information to the member device when the acquisition request
7 is received by the reception unit.

1 65. A member device that uses a content after registering 6
2 in a group managed by a group management device, comprising:
3 a selecting unit operable to select one of a plurality
4 of group management devices based a preset criterion;
5 a requesting unit operable to request the selected
6 group management device for registration to a group;
7 a receiving unit operable to receive, from the selected
8 group management device, common secret information unique
9 to the group; and
10 a holding unit operable to hold the received common
11 secret information, wherein
12 the preset criterion is, with respect to each group
13 management device, one of (i) a distance from the member
14 device, (ii) a communication time with the member device,
15 (iii) a processing capacity, and (iv) a processing state.

1 66. An authentication method used in a group management 7
2 device that manages a group, comprising the steps of:
3 receiving a request from a member device;
4 authenticating whether the member device is a

5 legitimate device, using common secret information unique
6 to the group and common secret information held by the member
7 device; and
8 judging the member device to be registered in the group
9 when authentication is successful.

1 67. A computer program used in a group management device that 4
2 manages a group, comprising the steps of:
3 receiving a request from a member device;
4 authenticating whether the member device is a
5 legitimate device, using common secret information unique
6 to the group and common secret information held by the member
7 device; and
8 judging the member device to be registered in the group
9 when authentication is successful.

1 68. A recording medium storing a computer program used in 9
2 a group management device that manages a group, the computer
3 program comprising the steps of:
4 receiving a request from a member device;
5 authenticating whether the member device is a
6 legitimate device, using common secret information unique
7 to the group and common secret information held by the member
8 device; and

9 judging the member device to be registered in the group
10 when authentication is successful.